Docket No.: 60468.300204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	**OLKIN et al.**		
Application No.:	**10/707,191**	Group No.:	**2137**
Filed:	**11/25/2003**	Examiner:	**GELAGAY, Shewaye**

For: **IMPLEMENTING NONREPUDIATION AND AUDIT USING AUTHENTICATION ASSERTIONS AND KEY SERVERS**

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. § 41.31)

This brief is in furtherance of the Notice of Appeal filed herewith.

The fees required under § 41.20, and any required petition for extension of time for filing this brief and fees there for, are dealt with concurrently in the Office's EFS-Web document submission tool.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(1)):

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Secure Data In Motion, Inc., a Delaware corporation of 1875 South Grant Street, Suite 850, San Mateo, CA 94402, which is assignee of the entire right, title and interest to the invention in the United States and in all foreign countries.

II RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences which may be related to, that will directly affect, or be directly affected by or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III STATUS OF CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The status of the claims in this application are:

A. TOTAL NUMBER OF CLAIMS IN THE APPLICATION

Claims in the application are: 1-27

B. STATUS OF ALL OF THE CLAIMS

1. Claims rejected: 1-27
2. Claims allowed or confirmed: NONE
3. Claims withdrawn from consideration: NONE
4. Claims objected to: NONE
5. Claims canceled: NONE
6. Accordingly, the pending claims are: 1-27

C. CLAIMS ON APPEAL

The claims on appeal are: 1-27

IV STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

Insofar as understood by the Appellant, all amendments have been acted upon and entered by the Examiner.

V SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

Appellants' invention comprises method and apparatus for a transaction source and a transaction target to exchange a transaction that cannot be repudiated (claims 1 and 19); for establishing a transaction as nonrepudiate able by a transaction source (claims 5 and 23), and establishing a transaction as nonrepudiate able by a transaction target/recipient (claims 14 and 26).

Appellants' FIG. 15 best depicts the claimed invention. Regrettably however, FIG. 9 is on the cover page of the published application but is not particularly relevant to the present claims. FIG. 9 more appropriately goes with the claims in related U.S. Pat. 7,277,549. For example, nothing in FIG. 9 represents an authentication assertion, where these come from, or how they are used. In contrast, FIG. 15 shows all of this and [0254]-[0263] describe it in detail.

As can be seen in FIG. 15, a trusted third-party system is employed. A source (414) and a key server (420) use an authentication authority (418) as a trusted third-party. Similarly, a target (416) and the key server (420) also use the authentication authority (418) as a trusted third-party. The source (414) and the target (416) are transacting parties (412) and a transaction (424) can be a message like an e-mail, an instant message, a video-conference, a collaborative document, etc. ([0007]). Of particular importance here is that such a message have a transactional character. That is, the fact that a message exists and is communicated is necessary but not especially relevant and even that the message is secured so that only the source and the target(s) know its contents is not especially relevant. Rather, what is important here is that the message establishes a transaction (e.g., a business event) between the transacting parties. For this non-repudiation and audit are important.

As the specification discusses at [0020]:

For example, when a financial brokerage company determines that a customer's margin call is due it must send the customer a notice. The brokerage company may follow up with a phone call. The ability of the business to determine if the customers have opened their notices impacts the process of calling the customers to follow up. In this example, if the business can prove that the customer has opened the notice, then it need not call the customer to follow up. This can result in a reduced number of customer follow up calls, which in turn translates into savings for the business.

Continuing with FIG. 15, and starting with a new or initial transaction, a transaction source (414) obtains an authentication assertion (422) from an authentication authority (418). In the case of a transaction source (414) this takes place at an early point (before any of the steps in claims 1 or 5).

The transaction source (414) then sends the authentication assertion (422) and various other information to the key server (420). This request may simply be a generalized request, or it may include a transaction ID (428) and/or a cryptography key (430). Although not germane to this appeal, such other information sent to the key server (420) can include sophisticated instructions, such as to not release the key to another party before a set time criteria, to not release the key after a set time criteria (i.e., to set a transaction expiration point), to release a key again only within a set period after a prior request, to not release key again within a set period after a prior request (e.g., accept offer within 24 hours or it may be extended to others), release the key only a set number of times, advise if the key is never requested, advise of the total number of times the key is requested, etc. Continuing, in the case of a simple request, the key server (420) can then provide the transaction ID (428) and the key (430) back to the transaction source (414). Alternately, the transaction source (414) may provide the key server (420) with the transaction ID (428) and the key (430), for the key server (420) to simply store for potential later use as described presently.

In either approach, the key server (420) verifies the source authentication assertion (422) and stores the transaction ID (428), the key (430), a time-stamp, and other information as desired.

The transaction source (414) prepares the transaction (424) by encrypting a message or simply by digitally signing an otherwise clear text (or "clear content") message using the key (430). It may have already done this if it is providing the transaction ID (428) and key (430) to the key server (420), or it can now do this if it has received these from the key server (420). Then the transaction source (414) sends the transaction (424) to the transaction target (416). Of course,

the transaction source (414) can use one key (430) for multiple transactions (424) or for sending one transaction (424) to multiple transaction sources (414), or the transaction source (414) can use multiple keys (430) for sending the same message to multiple transaction sources (414).

The transaction target (416) next receives the transaction (424), and it sends the transaction ID (428) and a target authentication assertion (422) to the key server (420). If the transaction target (416) does not have an authentication assertion (422), it can now simply get one. The transaction (424) may even list one or more authentication authorities (418) that are suitable because it is established that the key server (420) trusts them. Note also, the transaction ID (428) does not necessarily need to have reached the transaction target (416) in or with the transaction (424). For example, it may be sent separately between the transacting parties (412) or it may be based on an identifier of the transaction source (414) and a checksum generated from the message.

The key server (420) verifies the target authentication assertion (422) and uses the transaction ID (428) to determine whether it has the matching key (430). Of course, time-stamped audit records can be kept of all key requests regardless of verification, and notifications can be sent to the transaction source (414). Upon proper verification, the key server (420) sends the key (430) to the transaction target (416).

Then the transaction target (416) processes the transaction (428). This can be by decrypting the transaction (428), and/or verifying a signature in it, or simply by storing the transaction (428) and key (430) in case there ever is some dispute over the fact that there was a transaction (428), who was the source of it, or what the content of it was.

And that brings us back to non-repudiation. Lets continue with the example from the specification at [0020]. Say that brokerage Alice sends customer Bob a margin call transaction. If Bob receives the transaction and requests they key, the key server can inform Alice. If the key server does not release the key, which it should only do upon verification of an authentication assertion being provided by Bob, Alice can take more affirmative measures to contact Bob (and to sort out any technical issues relating to key release failure or any malicious ones, such as somebody hacking into Bob's e-mail account). More typically, when the key server does release the key Alice will know that her message arrived and was impliedly viewed by Bob. Any dispute over the facts can be resolved by auditing the records of the key server. Furthermore, any dispute over transaction content can be resolved by the use concurrently of a conventional tamper-

detection mechanism (e.g., transaction encryption and decryption or checksum comparison). With time-stamps used at the key server, the parties also cannot repudiate when the transaction was exchanged.

VI GROUND OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

A. Whether claims 1-27 are obvious over U.S. Patent Number 7,146,009 by Andivahis et al. (hereinafter Andivahis) in view of U.S. Publication Number 2004/0139319 by Favazza et al. (hereinafter Favazza), and thereby unpatentable under 35 U.S.C. § 103(a).

VII ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

> *To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.* MPEP §§ 706.02(j), 2143

VII(A) ARGUMENTS—PRELIMINARY COMMENTS

There are two major points of disagreement between the Examiner and Appellant.

The first is over message non-repudiation. A non-repudiate-able message is one that the sender cannot deny, either with respect to having sent it or with respect to its content. Appellant has pointed out that the:

> *claims are all directed to systems and methods to achieve message non-repudiation, and neither Andivahis or Favazza teach how to achieve non-repudiation ...* [and that] [t]*his begs the question, if none of the cited references teach non-repudiation, how can any combination of the cited references support rejection of Applicant's claims for non-repudiation systems and methods?* (08/24/2007 Response at pg. 5, ln. 24 through pg. 6, ln. 2)

The Examiner has merely argued in reply to this that Andivahis teaches that a request for a key with an "assertion" is verified by a trusted party, and noted other irrelevant details

(09/10/2007 advisory Action, 2nd to last ¶ on Continuation Sheet). Accordingly, it presently stands un rebutted that the cited references do not teach or reasonably suggest how to achieve message non-repudiation, and that the only such teaching of such that is of record in this case is Appellant's own specification.

The second major point of disagreement is over a key claim element, an authentication assertion. An authentication assertion is used in every step or is a sub-element in every element in every independent claim in this case. However, the Examiner still apparently does not understand what an authentication assertion is or how one is used. Appellant's FIG. 15 depicts authentication assertions and paragraph [0255] of the specification describes them:

> *the authentication authority **418** issues the transacting party **412** an authentication assertion **422**. ... The assertion **422** includes the identity of the transacting party **412**; the identity of the authentication authority **418**; the validity period of the authentication assertion **422**; and optional confirmation data, used by the key server **420** to prove that the transacting party **412** is the rightful owner of the assertion **422**.*

With this as context, it can be seen that the cited references do not teach or reasonably suggest authentication assertions, either alone or taken in combination.

The Examiner primarily relies on Andivahis as teaching a perceived equivalent to an authentication assertion, yet what Andivahis teaches comes from a different source (a key server vs. Appellant's authentication authority/server) and is used differently (for performing registration with the key server vs. authenticating one party to another with an existing authentication assertion). Notably, Andivahis' figures nowhere show anything arguably equivalent to Appellant's authentication authority and, as discussed below, its text does not disclose such either. Andivahis merely shows and discusses a key server. And Favazza does not teach either an authentication authority or a key server. The only element in it that is even superficially arguable in this respect is its policy server (56), and at [0033] it defines this as something not applicable here. Also, at [0030] Favazza shows that its handling of "authentication" is conventional and not applicable to Appellant's authentication authority and the authentication assertions this issues for use by other elements of the claimed invention.

VII(B) THE REJECTIONS UNDER 35 U.S.C. § 103(a) BASED ON THE COMBINATION OF ANDIVAHIS AND FAVAZZA ARE IMPROPER

VII(B)(i) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 1 (Or Dependant Claims 2-4)

VII(B)(i)(a) There Is No Reasonable Expectation Of Success

Claim 1 recites a "*method for a transaction source and a transaction target to exchange a transaction that cannot be repudiated.*" By definition, success here is non-repudiate-ability. But neither Andivahis, Favazza, or their combination teach or reasonably suggest how a message or transaction or anything can be made non-repudiate-able. The only counter remarks in this entire prosecution are a recitation of irrelevant details in the 09/10/2007 advisory Action, 2nd to last ¶ on Continuation Sheet.

VII(B)(i)(b) Andivahis And Favazza Do Not Teach Or Suggest All The Claim Limitations

Two key elements (limitations) in claim 1 are a source authentication assertion and a target authentication assertion. Neither Andivahis or Favazza teach or reasonably suggest either of these, and thus neither does their combination. For example, step (a) of claim 1 recites "*receiving a first request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion.*" Since this is the first step of the claimed method here, the source authentication assertion has to already exist to have been included in the request that is received here. The Examiner has cited (06/29/2007 office Action, pg. 5) Andivahis at col. 4, ln. 22-37 as teaching this. But what Andivahis actually describes here is:

> *an authentication process ... between* [a] *sender **210** and* [a] *key server ...* [wherein] *the sender sends an authentication request message to the key server and the latter responds with a number of strings of random bits, one such string for each such message to be sent to the key server.* (underline emphasis added)

Two things are particularly noteworthy here.

First, there is nothing equivalent to Appellant's authentication assertion in Andivahis' authentication request message. Andivahis does not recite anything equivalent here, and to understand why Andivahis does not need such one only has to look back to col. 4, ln. 16-22. Here we see that Andivahis' key server uses a database of registered users. Nothing Andivahis uses is equivalent to an authentication assertion from a trusted third party.

Second, Andivahis' strings of random bits are not authentication assertions. They are issued by the key server after a sender request, so there is a did the chicken or the egg come first

type problem here. Andivahis' bit strings also are for future messages to be sent to the key server (not messages to be sent from its sender to its recipient). Here it needs to be recalled that claim 1 is for a "*method for a transaction source and a transaction target to exchange a transaction.*" Granted, claim 1 does not recite that such a transaction cannot go via a key server, but one of ordinary skill in the art will readily appreciate that having messages and keys all pass via the same server seriously undermines security. Appellant's disclosure shows that this is unnecessary (see e.g., FIG. 15) and claim 1 here should not be construed in a manner that a skilled artisan would not employ (notably, one that Andivahis does not employ with its actual sender-recipient messages).

VII(B)(ii) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 5 (Or Dependant Claims 6-13)

Claim 5 includes a subset of the steps recited in claim 1. Specifically, it recites essentially the same steps (a)-(d) that apply to just the source side in a transaction exchange.

As such, Appellant's arguments above also apply here. The Andivahis-Favazza combination [1] does not provide a reasonable expectation of success and [2] does not teach or suggest all the claim limitations. Success by definition is transaction non-repudiation and nothing in the record here other than Appellant's own specification teaches how to achieve this. Similarly, we have shown that the cited references do not teach or reasonably suggest a source authentication assertion.

VII(B)(iii) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 14 (Or Dependant Claims 15-18)

Claim 14 also includes a subset of the steps recited in claim 1. Specifically, it recites as steps (a)-(d), rather than steps (e)-(h) of claim 1, that apply to just the target side in a transaction exchange.

As such, Appellant's arguments above apply here as well. The Andivahis-Favazza combination [1] does not provide a reasonable expectation of success and [2] does not teach or suggest all the claim limitations. Success here again, by definition, is transaction non-repudiation

and nothing in the record here other than Appellant's own specification teaches how to achieve this. Similarly, we have shown that the cited references do not teach or reasonably suggest a target authentication assertion.

VII(B)(iv) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 19 (Or Dependant Claims 20-22)

As a preliminary point, claim 19 is essentially an apparatus employing the method of claim 1, and thus is subject to the same rationale discussed above for claim 1. Again, the Examiner has based rejection on the Andivahis-Favazza combination where these references do not provide a reasonable expectation of success and they do not teach or suggest all of the claim limitations.

Furthermore, in claim 19 the recitation of apparatus limitations distinguishes Appellant's claimed invention from Andivahis and Favazza even more clearly. Andivahis teaches a key server that performs user registration and issues bit strings for use in later messages sent to that key server. Andivahis only works if there is registration at its key server (240). In contrast, claim 19 recites a key server, but one that receives an already existing authentication assertion. Registration with Appellant's key server is simply not necessary, because the authentication assertion is all that the key server needs to perform its job. Notably, Appellant's key server does not need to know about the source and target of a transaction beyond that an authentication authority is vouching for them. This can further enhance security, say, if the key server itself is compromised.

Andivahis' bit strings are also not equivalent to Appellant's authentication assertions. Andivahis bit strings are essentially receipts, and they thus are only acceptable with their issuer or some closely affiliated party. In contrast, Appellant's authentication assertions are acceptable by any number of non-affiliated key servers (or other entities). Appellant's authentication assertions are issued by trusted third parties. As long as a key server has reason to trust a authentication authority (e.g., a financial institution, major corporation, government branch, etc.), the key server has reason to trust such authentication assertions.

Favazza does not teach anything that changes this. The Examiner has noted that "*Favazza teaches a customer inserting an assertion, and a signature into an initial request to a web*

service. (page 1, paragraphs 9-10)" in the 06/29/2007 office Action, pg. 4, bottom ¶, but the "assertion" here is a session ticket ID used in a session with a web server. This is not equivalent to Appellant's authentication assertion in its contents, and especially not in its manner of use.

VII(B)(v) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 23 (Or Dependant Claims 24-25)

Claim 23 includes a subset of the elements recited in claim 19. Specifically, it recites a key server that is essentially able to work with just source authentication assertions as described in claim 19.

As such, Appellant's arguments above that the combination of Andivahis and Favazza do not provide a reasonable expectation of success and that these references do not teach or suggest all the claim limitations should apply here as well.

VII(B)(vi) A Prima Facie Case Of Obviousness Has Not Been Established For Claim 26 (Or Dependant Claim 27)

Claim 26 also includes a subset of the elements recited in claim 19. Specifically, it recites a key server that is essentially able to work just with target authentication assertions as described in claim 19.

As such, Appellant's arguments above that the combination of Andivahis and Favazza do not provide a reasonable expectation of success and that these references do not teach or suggest all the claim limitations should apply here as well.

VII(C) Summary

The Examiner has failed to establish at least two of the three major criteria of a prima facie case and Appellant's claims should therefore be allowed.

VIII CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal are:

1. A method for a transaction source and a transaction target to exchange a transaction that cannot be repudiated, the method comprising:

(a) receiving a first request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

(b) verifying said source authentication assertion;

(c) storing said transaction identifier and information from said source authentication assertion, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction;

(d) providing said transaction identifier in reply to said first request so that the transaction and said transaction identifier can be sent to the transaction target;

(e) receiving a second request for a decryption key to decrypt the transaction once it has been received by the transaction target, wherein said second request includes said transaction identifier and a target authentication assertion;

(f) verifying said target authentication assertion;

(g) storing information from said target authentication assertion with the transaction identifier; and

(h) providing said decryption key in reply to said second request so that the transaction can be decrypted, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction.

2. The method of claim 1, wherein said step (d) includes also providing an encryption key to encrypt the transaction.

3. The method of claim 1, the method further comprising:

(i) receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

(j) retrieving at least some of said information from said source authentication assertion stored in said step (c) with said transaction identifier and determining said source information therefrom; and

(k) providing said source information in reply to said information request.

4. The method of claim 1, the method further comprising:

(i) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target;

(j) determining if said information identifying the transaction target matches with any said information from said target authentication assertion stored with the transaction identifier stored in said step (g) and determining said target information therefrom; and

(k) providing said target information in reply to said information request.

5. A method for establishing a transaction as nonrepudiate able by a transaction source that is the origin of the transaction, the method comprising:

(a) receiving a request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

(b) verifying said source authentication assertion;

(c) storing said transaction identifier and information from said source authentication assertion; and

(d) providing said transaction identifier in reply to said request, thereby establishing information making the transaction source unable to plausibly repudiate being the origin of the transaction.

6. The method of claim 5, wherein said step (d) includes also providing an encryption key to encrypt the transaction.

7. The method of claim 5, the method further comprising:

(e) receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

(f) retrieving at least some of said information from said source authentication assertion stored in said step (c) with said transaction identifier and determining said source information therefrom; and

(g) providing said source information in reply to said information request.

8. The method of claim 7, wherein said source information indicates who the transaction source actually is.

9. The method of claim 7, wherein:

said information request received in said step (e) also includes information identifying a party believed to be the transaction source; and

said source information provided in said step (g) indicates merely whether said party is the transaction source, thereby responding to said information request without specifically identifying the transaction source.

10. The method of claim 7, wherein:

said step (c) includes also storing a decryption key usable to decrypt the transaction; and

said step (g) includes also providing said decryption key, thereby facilitating decryption of the transaction by a party making said information request even when said party is not the transaction source or a target of the transaction.

11. The method of claim 7, wherein:

said information request received in said step (e) also includes the transaction; and

said step (g) includes decrypting the transaction before providing said source information in reply to said information request.

12. The method of claim 11, wherein:

said information request received in said step (e) also includes information identifying a party believed to be the transaction source; and

said source information provided in said step (g) indicates merely whether said party is the transaction source, thereby responding to the second request without specifically identifying the transaction source.

13. The method of claim 11, wherein said step (g) includes also providing the transaction in decrypted form in said reply to said information request, thereby facilitating a party making said information request being able to confirm the content of the transaction even when said party is not the transaction source or a target of the transaction.

14. A method for establishing a transaction as nonrepudiate able by a transaction target that is a recipient of the transaction, wherein a transaction identifier identifying the transaction and a decryption key usable to decrypt the transaction have been pre-stored, the method comprising:

(a) receiving a request for the decryption key, wherein said request includes the transaction identifier and a target authentication assertion;

(b) verifying said target authentication assertion;

(c) storing information from said target authentication assertion with the transaction identifier; and

(d) providing the decryption key in reply to said request, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction.

15. The method of claim 14, the method further comprising:

(e) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target;

(f) retrieving at least some of said information from said target authentication assertion stored in said step (c) with said transaction identifier and determining said target information therefrom; and

(g) providing said target information in reply to said information request.

16. The method of claim 15, wherein:

said step (g) includes also providing said decryption key, thereby facilitating decryption of the transaction by a party making said information request even when said party is not the transaction source or a transaction target.

17. The method of claim 15, wherein:

said information request received in said step (e) also includes the transaction; and

said step (g) includes decrypting the transaction before providing said identity information.

18. The method of claim 17, wherein said step (g) includes also providing the transaction in decrypted form in said reply to said information request, thereby facilitating a party making said information request being able to confirm the content of the transaction even when said party is not the transaction source or a transaction target.

19. A system for a transaction source and a transaction target to exchange a transaction that cannot be repudiated, comprising:

a computerized key server;

said key server suitable for receiving a first request via a network for a transaction identifier to identify the transaction, wherein said first request includes a source authentication assertion;

said key server suitable for receiving a second request via said network for a decryption key usable to decrypt the transaction, wherein said second request includes said transaction identifier and a target authentication assertion;

said key server suitable for verifying said source authentication assertion and said target authentication assertion;

said key server suitable for storing said transaction identifier, information from said source authentication assertion, and information from said target authentication in association in a database;

said key server suitable for providing a first reply to said first request via said network that includes said transaction identifier; and

said key server suitable for providing a second reply to said second request via said network that includes said decryption key, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction and also making the transaction target unable to plausibly repudiate once it is provided said decryption key.

20. The system of claim 19, wherein said key server is further suitable for providing an encryption key to encrypt the transaction in said first reply.

21. The system of claim 19, wherein:

said key server is further suitable for receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

said key server is further suitable for retrieving said information from said source authentication assertion stored with said transaction identifier from said database and determining said source information therefrom; and

said key server is further suitable for providing said source information in reply to said information request.

22. The system of claim 19, wherein:

said key server is further suitable for receiving an information request for target, wherein said information request includes said transaction identifier and information identifying the transaction target;

said key server is further suitable for determining if said information identifying the transaction target matches with any said information from said target authentication assertion stored with the transaction identifier and determining said target information therefrom; and

said key server is further suitable for providing said target information in reply to said information request.

23. A system for establishing a transaction as nonrepudiate able by a transaction source that is the origin of the transaction, comprising:

a computerized key server;

said key server suitable for receiving a request via a network for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

said key server suitable for verifying said source authentication assertion;

said key server suitable for storing said transaction identifier and information from said source authentication assertion in a database; and

said key server suitable for providing a reply via said network that includes said transaction identifier, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction.

24. The system of claim 23, wherein said key server is further suitable for providing an encryption key to encrypt the transaction in said reply.

25. The system of claim 23, wherein:

said key server is further suitable for receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

said key server is further suitable for retrieving information from said source authentication assertion stored with said transaction identifier from said database, and determining said source information therefrom; and

said key server is further suitable for providing said source information in reply to said information request.

26. A system for establishing a transaction as nonrepudiate able by a transaction target that is a recipient of the transaction, wherein a transaction identifier identifying the transaction and a decryption key usable to decrypt the transaction have been pre-stored in a database, comprising:

a computerized key server;

said key server suitable for receiving a request via a network for the decryption key, wherein said request includes the transaction identifier and a target authentication assertion;

said key server suitable for verifying said target authentication assertion;

said key server suitable for storing information from said target authentication assertion with the transaction identifier in the database; and

said key server suitable for providing a reply via said network that includes the decryption key, thereby establishing information making the transaction target unable to plausibly repudiate.

27. The system of claim 26, wherein:

said key server is further suitable for receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target;

said key server is further suitable for retrieving at least some of said information from said target authentication assertion stored with said transaction identifier and determining said target information therefrom; and

said key server is further suitable for providing said target information in reply to said information request.

IX EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

None.

X RELATED PROCEEDINGS APPENDIX
(37 C.F.R. § 41.37(c)(1)(x))

None.

Patent Venture Group
10788 Civic Center Drive, Suite 215
Rancho Cucamonga, California 91730-3805

Respectfully Submitted,

Telephone: (909) 748-5145
Facsimile: (888) 847-2501
E-mail 1: RRoberts@pvglaw.com
E-mail 2: RRoberts@ipvglaw.com

Raymond E. Roberts
Reg. No.: 38,597